(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 923 054 A2

(12) EUROPÄISCHE PATENTANMELDUNG

(43) Veröffentlichungstag:
16.06.1999 Patentblatt 1999/24

(51) Int. Cl.[6]: **G07C 9/00**

(21) Anmeldenummer: **98122611.1**

(22) Anmeldetag: **27.11.1998**

(84) Benannte Vertragsstaaten:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Benannte Erstreckungsstaaten:
AL LT LV MK RO SI

(30) Priorität: **10.12.1997 DE 19754710**
06.04.1998 DE 19815300

(71) Anmelder:
F + G Megamos Sicherheitselektronik GMBH
51674 Wiehl (DE)

(72) Erfinder:
- **Petsching, Wilfried**
  51702 Bergneustadt (DE)
- **Marquart, Michael**
  59192 Bergkamen (DE)
- **Schenk, Christoph**
  51688 Wipperfürth (DE)
- **Seifert, Wolfgang**
  51647 Gummersbach-Lantenbach (DE)

(74) Vertreter: **Cohausz & Florack**
Patentanwälte
Kanzlerstrasse 8a
40472 Düsseldorf (DE)

(54) Verfahren und Vorrichtung zur Prüfung der Nutzungsberechtigung für Zugangskontrolleinrichtungen

(57) Die Erfindung betrifft ein Verfahren und eine Vorrichtung zur Prüfung der Nutzungsberechtigung für Zugangskontrolleinrichtungen und insbesondere für Schließeinrichtungen von Fahrzeugen, mit Hilfe einer zugangsseitigen Steuereinrichtung und mit Hilfe mindestens einer benutzerseitigen Identifikationseinrichtung, bei welchem zwischen der Steuereinrichung und einer Identifikationseinrichtung Autorisierungssignale ausgetauscht werden und bei welchem die in Reichweite der Steuereinrichtung befindlichen Identifikationseinrichtungen automatisch zur Übertragung der Autorisierungssignale angesprochen werden. Zur Vermeidung von Kollisionen der von verschiedenen Identifikationseinrichtungen übertragenen Autorisierungssignale ist vorgesehen, daß von der Steuereinrichtung ein Selektionssignal ausgesandt wird, und daß von einer Identifikationseinrichtung nach dem Empfang eines ausschließlich dieser Identifikationseinrichtung zuzuordnenden Selektionssignals das Autorisierungssignal ausgesendet wird.

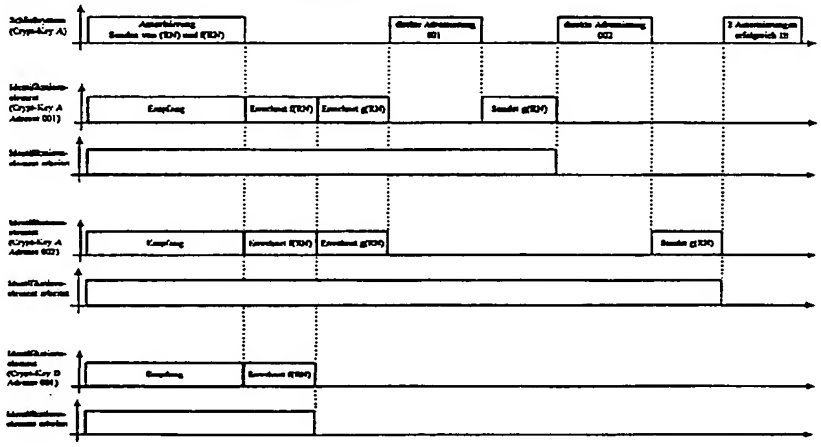

Fig. 2

EP 0 923 054 A2

Beschreibung

[0001] Die Erfindung betrifft ein Verfahren und eine Vorrichtung zur Prüfung der Nutzungsberechtigung für Zugangskontrolleinrichtungen, insbesondere für Schließeinrichtungen von Fahrzeugen, mit Hilfe einer zugangsseitigen Steuereinrichtung und mit Hilfe mindestens einer benutzerseitigen Identifikationseinrichtung, bei welchem zwischen der Steuereinrichtung und einer Identifikationseinrichtung Autorisierungssignale ausgetauscht werden und bei welchem die in Reichweite der Steuereinrichtung befindlichen Identifikationseinrichtungen automatisch zur Übertragung der Autorisierungssignale angesprochen werden.

[0002] Ein Verfahren bzw. eine Vorrichtung dieser Art kommt immer dann zum Einsatz, wenn es um die Überprüfung geht, ob eine bestimmte Person als Inhaber der Identifikationseinrichtung autorisiert ist, die Zugangskontrolleinrichtung zu passieren. Dies gilt sowohl für ortsfeste Zugangskontrolleinrichtungen, zu denen nur ein ausgewählter Personenkreis Zutritt hat, als auch für mobile Zugangskontrolleinrichtungen, insbesondere an Fahrzeugen, wie Kraftfahrzeugen, Schiffen oder Fahrrädern. Durch das Vorsehen von Zugangskontrolleinrichtungen soll hier dem Diebstahl des Fahrzeugs entgegengewirkt werden. Die Vorrichtung setzt sich dabei zusammen aus den beiden Grundkomponenten, zum einen der zentral angeordneten Steuereinrichtung, welche in der Regel dauerhaft mit Energie versorgt ist, und zum anderen den mobilen Identifikationseinrichtungen, die den autorisierten Benutzer identifizieren sollen. Die Identifikationseinrichtung kann dabei selbst Teil eines Fahrzeugschlüssels sein, welcher mit der Steuereinrichtung im Bereich der Schließanlage des Fahrzeuges in vorzugsweise bidirektionalem Datenaustausch steht.

[0003] Den heutigen Stand der Technik für die beschriebenen Identifikationseinrichtungen bilden sog. in Fahrzeugschlüsseln, Chipkarten oder dergleichen integrierte Transponder. Derartige Transponder weisen keine eigene Energieversorgung auf, sondern werden bei der Annäherung der Identifikationseinrichtung an die Steuereinrichtung drahtlos mit Energie versorgt und im weiteren automatisch zur Übertragung der Autorisierungs-signale angesprochen.

[0004] Verfahren bzw. Vorrichtungen zur Prüfung der Nutzungsberechtigung, von denen die vorliegende Erfindung ausgeht, sind aus der Praxis im Anwendungsbereich für Fahrzeuge bekannt. Im einfachsten Fall handelt es sich um ein elektromagnetisches Identifizierungssystem bestehend aus einem im Zündschlüssel integrierten passiven Datenträger in Form eines Transponders sowie einer vorzugsweise am Zündschloß angebrachten Antennenspule, die mit der Steuereinrichtung verbunden ist. Ein solches System wird in der Regel über den Zündkontakt des Fahrzeuges aktiviert, wodurch das Steuergerät ein magnetisches Wechselfeld aussendet. Dieses regt den Datenträger im Transponder zum Aussenden seiner fest abgespeicherten Dateninformation an. Die Tendenz geht bei modernen Zugangskontrolleinrichtungen allerdings zunehmend dahin, daß die Identifikationseinrichtungen bereits in einigem Abstand von der Steuereinrichtung angesprochen werden, ohne daß ein mechanisches Inverbindungtreten zwischen der Identifikationseinrichtung und der Steuereinrichtung notwendig ist. Die von der Steuereinrichtung empfangenen Daten der Identifikationseinrichtung werden in der Steuereinrichtung demoduliert und mit einer in einer Schlüsseltabelle abgelegten Vorgabeinformation verglichen. Nur im Falle einer Übereinstimmung kann das Fahrzeug gestartet werden.

[0005] Eine weitere Vorrichtung bzw. ein weiteres Verfahren zur Prüfung der Nutzungsberechtigung für Fahrzeuge ist das aus der Praxis ebenfalls bekannte sog. "Challenge-and-Response-Verfahren". Hierbei sendet die Steuereinrichtung zunächst an die Identifikationseinrichtung eine beliebige Dateninformation. Diese wird in der Identifikationseinrichtung mit einem geheimen Schlüssel unter Verwendung einer Verschlüsselungsfunktion verschlüsselt. Die verschlüsselte Information wird an die Steuereinrichtung zurückgesendet. Die Steuereinrichtung wendet nun auf die empfangene Nachricht die Inversfunktion zur Verschlüsselungsfunktion in Verbindung mit dem geheimen Schlüssel an. Die dadurch erzeugte Information wird in der Steuereinrichtung verglichen mit der ursprünglich erzeugten Ausgangsfunktion. Wenn eine Übereinstimmung vorliegt, wird die Nutzungsberechtigung als gegeben angesehen.

[0006] Neben diesem aus der Praxis bekannten Stand der Technik ist aus der auf die Anmelderin zurückgehenden DE 195 23 009 A1 ein Verfahren bzw. eine Vorrichtung zur Prüfung der Nutzungsberechtigung für Zugangskontrolleinrichtungen bekannt, bei dem zunächst eine in der Steuereinrichtung erzeugte und von dort zur Identifikationseinrichtung übertragene unverschlüsselte Zahlenfolge und eine ebenfalls in der Steuereinrichtung aus der unverschlüsselten Zahlenfolge anhand eines geheimen Schlüssels erzeugte verschlüsselte Zahlenfolge an die Identifikationseinrichtung übertragen werden. Die Identifikationseinrichtung berechnet anschließend mit der in ihr gespeicherten inversen Verschlüsselungsfunktion aus der verschlüsselten Zahlenfolge eine dritte Zahlenfolge und vergleicht diese mit der übertragenen unverschlüsselten Zahlenfolge. Bei dem bekannten Verfahren wird bei Feststellung einer mangelnder Übereinstimmung der Zahlenfolgen die Berechtigungsprüfung abgebrochen. Wird hingegen eine Übereinstimmung festgestellt, so sendet die Identifikationseinrichtung anschließend eine weiter verschlüsselte Zahlenfolge aus, die in der Identifikationseinrichtung aus der verschlüsselten Zahlenfolge und dem gespeicherten geheimen Schlüssel erzeugt wird. Diese als Autorisierungssignal an die Steuereinrichtung übermittelte dritte Zahlenfolge wird

von der Steuereinrichtung invers verschlüsselt und mit der aus der unverschlüsselten Zahlenfolge erzeugten verschlüsselten Zahlenfolge verglichen. Liefert dieser Vergleich eine Übereinstimmung der verglichenen Zahlenfolgen, so wird die Zugangskontrolleinrichtung freigegeben.

[0007] Problematisch ist bei den aus dem Stand der Technik bekannten Verfahren und Vorrichtungen zur Prüfung der Nutzungsberechtigung für Zugangskontrolleinrichtungen, bei denen die in Reichweite der Steuereinrichtung befindlichen Identifikationseinrichtungen automatisch zur Übertragung der Autorisierungssignale angesprochen werden, daß eine relativ große Wahrscheinlichkeit dafür besteht, daß gleichzeitig mehrere Identifikationseinrichtungen in die Reichweite der Steuereinrichtung gelangen. Diese Identifikationseinrichtungen werden nun von der Steuereinrichtung unabhängig davon, ob sie dem jeweiligen Schließsystem zuzuordnen sind, angesprochen. Hierbei kann es im wesentlichen zu zwei Arten von Störungen kommen. Zum einen können Identifikationseinrichtungen gleichzeitig angesprochen werden, die verschiedenen Schließsystemen zugeordnet sind. Dies tritt beispielsweise auf, wenn sich Fahrer und Beifahrer einem Kraftfahrzeug nähern, wobei der Fahrer eine zur Zugangskontrolleinrichtung des Kraftfahrzeuges zugehörige Identifikationseinrichtung bei sich trägt, während der Beifahrer eine zur Zugangskontrolleinrichtung eines anderen Kraftfahrzeuges zugehörige Identifikationseinrichtung bei sich trägt. Werden nun von der Steuereinrichtung beide Identifikationseinrichtungen angesprochen, so antworten beide Identifikationseinrichtungen mehr oder weniger gleichzeitig, wodurch es zu einer Überlagerung der von den Identifikationseinrichtungen ausgesandten Signale kommt, die durch die Kollision der elektromagnetischen Signale zu einer vollständigen Störung der Übertragung von Autorisierungssignalen führt. Diese Kollisionen treten auch bei den in der DE 195 23 009 A1 beschriebenen Verfahren auf, da hier die Identifikationseinrichtung bei Feststellung einer fehlenden Übereinstimmung zwischen der übertragenen verschlüsselten Zahlenfolge und der aus der übertragenen unverschlüsselten Zahlenfolge anhand des geheimen Schlüssels innerhalb der Identifikationseinrichtung erzeugten verschlüsselten Zahlenfolge ein Signal NACK(Not Acknowledged) und anschließend LW's (Listen windows) ausgesandt werden, um die Bereitschaft der Identifikationseinrichtung zur erneuten Autorisierung zu signalisieren. Zum anderen können Störungen der Autorisierung auch dann auftreten, wenn sich zwei Personen, insbesondere Fahrer und Beifahrer eines Kraftfahrzeugs, der Zugangskontrolleinrichtung nähern und beide Personen im Besitz einer Identifikationseinrichtung sind, die zur Freigabe der Zugangskontrolleinrichtung geeignet sind. Obwohl beide Identifikationseinrichtungen für sich eine Freigabe der Zugangskontrolleinrichtung ermöglichen, wird bei einer in etwa gleichzeitigen Annäherung der Identifikationseinrichtungen an die Steuereinrichtung aufgrund der im wesentlichen gleichzeitigen automatischen Ansprache der Identifikationseinrichtungen zur Übertragung der Autorisierungssignale diese Übertragung massiv gestört oder sogar unmöglich gemacht. Im Ergebnis läßt sich in einem solchen Fall die Freigabe der Zugangskontrolleinrichtung nur dadurch gewährleisten, daß eine der Identifikationseinrichtungen aus dem Einflußbereich der Steuereinrichtung herausbewegt wird. Beide Arten von Störungen sind offensichtlich unerwünscht, da sie eine Freigabe der Zugangskontrolleinrichtung durch autorisierte Identifikationseinrichtungen verhindern.

[0008] Ausgehend von den Problemen mit den aus dem Stand der Technik bekannten Verfahren und Vorrichtungen zur Prüfung der Nutzungsberechtigung für Zugangskontrolleinrichtungen liegt der Erfindung die Aufgabe zugrunde, ein Verfahren und eine Vorrichtung zur Prüfung der Nutzungsberechtigung für Zugangskontrolleinrichtungen zur Verfügung zu stellen, mit dem bzw. der eine störungsfreie Übertragung der Autorisierungssignale auch bei gleichzeitiger Annäherung mehrerer Identifikationseinrichtungen an eine Steuereinrichtung gewährleistet ist.

[0009] Die zuvor hergeleitete und aufgezeigte Aufgabe wird gemäß einer ersten Lehre der Erfindung bei einem Verfahren zur Prüfung der Nutzungsberechtigung für Zugangskontrolleinrichtungen dadurch gelöst, daß von der Steuereinrichtung ein Selektionssignal ausgesendet wird und daß von einer Identifikationseinrichtung nach dem Empfang eines ausschließlich dieser Identifikationseinrichtung zuzuordnenden Selektionssignals das Autorisierungssignal ausgesendet wird. Durch diese Maßnahmen gemäß der ersten Lehre der Erfindung ist also gewährleistet, daß die Identifikationseinrichtung nur dann ein Autorisierungssignal aussendet, wenn sie eindeutig angesprochen ist. Entsprechend können also keine gegenseitigen Störungen der Autorisierungssignale gemäß der ersten Lehre der Erfindung ausgestalteter Identifikationseinrichtungen mehr auftreten. Bei dem nach der ersten Lehre der Erfindung ausgestalteten Verfahren werden selbstverständlich auch verschiedenen Identifikationseinrichtungen, die ein und derselben Zugangskontrolleinrichtung zugeordnet sind, verschiedene Selektionssignale zugeordnet. Die nach der ersten Lehre der Erfindung vorgesehene Ausschließlichkeit bzw. Eindeutigkeit der Zuordnung des Selektionssignals bewegt sich in dem für Zugangskontrolleinrichtungen üblichen Rahmen.

[0010] Eine besonders vorteilhafte Ausgestaltung erfährt die erste Lehre der Erfindung dadurch, daß die Autorisierungssignale bidirektional zwischen der Steuereinrichtung und den Identifikationseinrichtungen übertragen werden, und daß die von der Steuereinrichtung ausgesandten Autorisierungssignale einen Teil des Selektionssignals bilden. Der zusätzliche Aufwand für die Auswahl eines nur einer Identifikationseinrichtung zugeordneten Selektionssignals läßt sich durch die soeben beschriebene Maßnahme entscheidend redu-

zieren. Bei einem nach der beschriebenen Ausgestaltung arbeitenden Verfahren wird bei Verfahren zur Prüfung der Nutzungsberechtigung für Zugangskontrolleinrichtungen, die nach dem "Challenge-and-Response-Verfahren" arbeiten, die von der Steuereinrichtung an die Identifikationseinrichtung übertragene Dateninformation gleichzeitig zur Übertragung eines Teils des Selektionssignals genutzt.

[0011] Die beschriebene Ausgestaltung eines Verfahrens nach der ersten Lehre der Erfindung läßt sich besonders vorteilhaft mit dem aus der DE 195 23 009 A1 bekannten Verfahren dadurch verknüpfen, daß in der Steuereinrichtung eine Zahlenfolgen und aus der Zahlenfolge eine verschlüsselte Zahlenfolge erzeugt wird, daß die Zahlenfolge und die verschlüsselte Zahlenfolge als Autorisierungssignal an die Identifikationseinrichtung übertragen wird, daß in der Identifikationseinrichtung die verschlüsselte Zahlenfolge invers verschlüsselt und mit der Zahlenfolge verglichen wird und daß aus der Übereinstimmung der verglichenen Zahlenfolgen zumindest ein Teil des Selektionssignals abgeleitet wird. Nach dieser Ausgestaltung läßt sich also die bekannte Übertragung einer unverschlüsselten und einer verschlüsselten Zahlenfolge von der Steuereinrichtung an eine Identifikationseinrichtung, die ursprünglich zur Verbesserung der Sicherheit der Nutzungsberechtigungsprüfung vorgesehen war, gleichzeitig zur Selektion der in der Reichweite der Steuereinrichtung befindlichen Identifikationseinrichtungen verwenden. Bei dieser Ausgestaltung lassen sich Störungen selbstverständlich nur vermeiden, wenn im Unterschied zum Stand der Technik darauf verzichtet wird, daß die Identifikationseinrichtung bei mangelnder Übereinstimmung der zu vergleichenden Zahlenfolgen kein NACK und keine LW's aussendet, die wiederum zu Kollisionen in der Datenübertragung führen würden. Die angesprochenen Identifikationseinrichtungen, bei denen der Vergleich keine Übereinstimmung ergibt, schweigen im Anschluß an den Vergleich.

[0012] Bei der Vervollständigung des Verfahrens zur Prüfung der Nutzungsberechtigung für Zugangskontrolleinrichtungen gemäß der ersten Lehre der Erfindung ist es des weiteren vorteilhaft, daß das nach Feststellung der Übereinstimmung der verglichenen Zahlenfolgen von der Identifikationseinrichtung an die Steuereinrichtung übertragene Autorisierungssignal aus der Zahlenfolge oder der verschlüsselten Zahlenfolge durch weitere Verschlüsselung erzeugt wird und daß bei Übereinstimmung des in der Steuereinrichtung invers verschlüsselten Autorisierungssignals der Identifikationseinrichtung mit der Zahlenfolge oder der verschlüsselten Zahlenfolge die Zugangskontrolleinrichtung freigegeben wird. Diese Maßnahme ermöglicht die Verwirklichung des in der DE 195 23 009 A1 beschriebenen Verfahrens bei gleichzeitiger teilweiser oder vollständiger Selektion der Identifikationseinrichtungen.

[0013] Um mit den bislang beschriebenen Maßnahmen eine vollständige Selektion der Identifikationseinrichtungen zu gewährleisten, sind für verschiedene, einer Zugangskontrolleinrichtung zugeordnete Identifikationseinrichtungen verschiedene geheime Schlüssel erforderlich. Dies ist zum einen aufwendig und zum anderen hinsichtlich der Erweiterung auf weitere der Zugangskontrolleinrichtung zugeordnete Identifikationseinrichtungen problematisch, da für jede Zugangskontrolleinrichtung eine gewisse Anzahl von geheimen Schlüsseln vorzuhalten wäre. Diese Problematik läßt sich dadurch vermeiden, daß gemäß einer weiteren Ausgestaltung der ersten Lehre der Erfindung zumindest ein Teil des Selektionssignals als eine einer Identifikationseinrichtung zugeordnete Zahlenfolge übertragen wird. Es ist nun zum einen möglich, jeder Identifikationseinrichtung, unabhängig davon, welcher Zugangskontrolleinrichtung sie zugeordnet ist, eine einmalige Zahlenfolge zuzuordnen. Besonders vorteilhaft ist jedoch die Verknüpfung der teilweisen Ableitung des Selektionssignals aus den Autorisierungssignalen mit einer Ergänzung des Selektionssignals durch eine Zuordnung einer einmaligen Zahlenfolge zu jeder einer gemeinsamen Zugangskontrolleinrichtung zugeordneten Identifikationseinrichtung. Eine derartige Aufteilung des Selektionssignals auf das Autorisierungssignal und eine uncodiert übertragbare Zahlenfolge ergibt eine besonders vorteilhafte Möglichkeit einer eindeutigen Selektion von Identifikationseinrichtungen.

[0014] Für eine Vorrichtung zur Prüfung der Nutzungsberechtigung für Zugangskontrolleinrichtungen ist die oben hergeleitete und aufgezeigte Aufgabe nach einer zweiten Lehre der Erfindung dadurch gelöst, daß die Steuereinrichtung ein Selektionssignal aussendet und daß eine Identifikationseinrichtung ein Autorisierungssignal nach dem Empfang eines ausschließlich dieser Identifikationseinrichtung zuzuordnenden Selektionssignals aussendet.

[0015] Eine Vorrichtung zur Prüfung der Nutzungsberechtigung für Zugangskontrolleinrichtungen gemäß der zweiten Lehre der Erfindung eignet sich neben ihrem möglichen Einsatz in stationären Zugangskontrolleinrichtungen, beispielsweise in Zugangsbereichen großer Firmen, besonders vorteilhaft zum Einsatz in Verbindung mit mobilen Zugangskontrolleinrichtungen, wobei die Identifikationseinrichtung einen insbesondere als Transponder ausgebildeten Teil eines Fahrzeugschlüssels bildet.

[0016] Es besteht nun eine Vielzahl von Möglichkeiten, das erfindungsgemäße Verfahren bzw. die erfindungsgemäße Vorrichtung zur Prüfung der Nutzungsberechtigung für Zugangskontrolleinrichtungen auszugestalten und weiterzubilden. Dazu wird einerseits auf die den Patentansprüchen 1 und 6 nachgeordneten Patentansprüche sowie andererseits auf die Beschreibung eines bevorzugten Ausführungsbeispiels in Verbindung mit der Zeichnung verwiesen. In der Zeichnung zeigen

Fig. 1 ein Funktionsschema eines bekannten Verfahrens zur Prüfung der Nutzungsberechtigung für Zugangskontrolleinrichtungen und

Fig. 2 schematisch ein Ausführungsbeispiel eines erfindungsgemäßen Verfahrens zur Prüfung der Nutzungsberechtigung für Zugangskontrolleinrichtungen.

[0017] Bei dem in Fig. 1 dargestellten bekannten Verfahren zur Prüfung der Nutzungsberechtigung für Zugangskontrolleinrichtungen sendet die als Schließsystem ausgebildete Steuereinrichtung einen Autorisierungsbefehl, der eine Zufallszahl (RN) und das durch Verschlüsselung der Zufallszahl mit Hilfe des geheimen Schlüssels Crypt-key errechnete Crypt-Zwischenergebnis f (RN) enthält. Das Identifikationselement errechnet seinerseits aus der Zufallszahl (RN) und seinem Crypt-key ein Crypt-Zwischenergebnis f (RN), welches es mit dem Zwischenergebnis des Schließsystems vergleicht. Sind beide Crypt-keys gleich, ergeben sich auch gleiche Zwischenergebnisse. In diesem Fall errechnet das Identifikationselement das Endergebenis g (RN) aus dem Zwischenergebnis f (RN) und der Anwendung des Crypt-keys und sendet es zurück zum Schließsystem, welches seinerseits ebenfalls aus f (RN) und seinem Crypt-key ein g (RN) errechnet hat.

[0018] Sind beide g (RN) gleich, ist die Autorisierung erfolgreich abgeschlossen. Sollte der Vergleich des Zwischen- oder Endergebnisses bei dem bekannten Verfahren zur Prüfung der Nutzungsberechtigung für Zugangskontrolleinrichtungen ein negatives Ergebnis liefern, so wird der Autorisierungsvorgang abgebrochen, und das Identifikationselement sendet ein NACK (Not-Acknowledged) und anschließend LW's (Listen Windows), um seine Bereitschaft zur erneuten Autorisierung zu signalisieren.

[0019] Bei dem aus dem Stand der Technik bekannten Verfahren zur Prüfung der Nutzungsberechtigung für Zugangskontrolleinrichtungen würden diese im Fehlerfall gesendeten Daten mit einem sich ebenfalls in Reichweite des Schließsystems befindenden Identifikationselement, welches gerade ein Endergebnis g (RN) sendet, kollidieren. Ebenso kollidieren die Daten von zwei oder mehr Identifikationselementen, wenn sie gleichzeitig die Endergebnisse g (RN) oder NACK's und LW's zurücksenden. Die Ursache für diese möglichen Kollisionen liegt in der autarken und unsynchronisierten Arbeitsweise jedes einzelnen Identifikationselementes, die erfindungsgemäß verändert wird.

[0020] Das in Fig. 2 dargestellte Ausführungsbeispiels des erfindungsgemäßen Verfahrens zur Prüfung der Nutzungsberechtigung für Zugangskontrolleinrichtungen arbeitet prinzipiell nach dem in Fig. 1 dargestellten Ablaufschema. Im obersten Diagramm in Fig. 2 sind die Aktionen eines nach dem erfindungsgemäßen Verfahren arbeitenden Schließsystems dargestellt. In den in Fig. 2 dargestellten 2., 3. und 4. Diagrammpaaren sind die Aktionen von erfindungsgemäß arbeitenden Identifikationselementen, wie im obersten Diagramm auf der Zeitachse, dargestellt.

[0021] Bei dem in Fig. 2 dargestellten Ausführungsbeispiel eines erfindungsgemäßen Verfahrens sendet das Schließsystem ein Autorisierungssignal, das eine Zufallszahl (RN) und ein Crypt-Zwischenergebnis f (RN) beinhaltet. Dieses Signal können praktisch alle Identifikationselemente, die sich in der Reichweite des Schließsystems befinden, empfangen und errechnen ihrerseits aus der Zufallszahl (RN) und ihren Crypt-keys ein f (RN). Besitzen nun das Schließsystem und das Identifikationselement den gleichen Crypt-key, stimmen auch beide f (RN) überein. Dies bedeutet, daß das Identifikationselement mit dem gleichen f (RN) zu dem Schließsystem, welches das Autorisierungssignal gesendet hat, gehört. Die in der zweiten und dritten Diagrammgruppe beschriebenen Identifikationselemente haben also den ersten Teil des Selektionssignals empfangen, der ihnen signalisiert, daß sie weiter aktiv bleiben sollen. Das in der vierten Diagrammgruppe dargestellte Identifikationselement, bei dem das Zwischenergebnis f (RN) nicht übereinstimmt, schaltet sich erfindungsgemäß, ohne Abgabe von NACK's und LW's ab, da es anhand des ersten Teils des Selektionssignals, das vorliegend von dem Autorisierungssignal gebildet wird, erkannt hat, daß es nicht von dem Schließsystem angesprochen wird.

[0022] Die Endergebnisse g (RN) werden von den noch aktiven Identifikationselementen, bei denen der erste Teil des Selektionssignals als ihnen zugeordnet bewertet worden ist, erst gesendet, wenn sie mit ihrer ergänzenden Identifikationselement-Adresse 001 oder 002 direkt angesprochen werden. Durch die Sendung der Endergebnisse g (RN) werden schließlich die Autorisierungen ohne Kollisionen abgeschlossen und die Zugangskontrolleinrichtung freigegeben.

[0023] Durch den oben beschriebenen Vorgang wird bereits während der Autorisierung eine Selektion der sich in Reichweite des Schließsystems befindlichen Identifikationselemente vorgenommen, so daß bei der abschließenden Selektion immer nur die zum Schließsystem gehörenden Identifikationselemente, deren Selektionsadresse bekannt und auch nur einmal innerhalb eines Schließsystems vorkommt, antworten. Das Autorisierungssignal vermeidet somit als Teil des Selektionssignals Kollisionen mit Identifikationselementen fremder Schließsysteme und die abschließende Selektion durch direkte Adressierung der einem Schließelement zugeordneten Identifikationselemente vermeidet die Kollisionen von einem Schließsystem zugeordneten Identifikationselementen untereinander.

Patentansprüche

1. Verfahren zur Prüfung der Nutzungsberechtigung für Zugangskontrolleinrichtungen, insbesondere für Schließeinrichtungen von Fahrzeugen, mit Hilfe

einer zugangsseitigen Steuereinrichtung und mit Hilfe mindestens einer benutzerseitigen Identifikationseinrichtung, bei welchem zwischen der Steuereinrichung und einer Identifikationseinrichtung Autorisierungssignale ausgetauscht werden und bei welchem die in Reichweite der Steuereinrichtung befindlichen Identifikationseinrichtungen automatisch zur Übertragung der Autorisierungssignale angesprochen werden,
dadurch gekennzeichnet, daß
von der Steuereinrichtung ein Selektionssignal ausgesandt wird, und daß von einer Identifikationseinrichtung nach dem Empfang eines ausschließlich dieser Identifikationseinrichtung zuzuordnenden Selektionssignals das Autorisierungssignal ausgesendet wird.

2. Verfahren nach Anspruch 1,
dadurch gekennzeichnet, daß
die Autorisierungssignale bidirektional zwischen der Steuereinrichtung und den Identifikationseinrichtungen übertragen werden und daß die von der Steuereinrichtung ausgesandten Autorisierungssignale einen Teil des Selektionssignals bilden.

3. Verfahren nach Anspruch 2,
dadurch gekennzeichnet, daß in
der Steuereinrichtung eine Zahlenfolge und aus der Zahlenfolge eine verschlüsselte Zahlenfolge erzeugt wird, daß die Zahlenfolge und die verschlüsselte Zahlenfolge als Autorisierungssignal an die Identifikationseinrichtung übertragen wird, daß in der Identifikationseinrichtung die verschlüsselte Zahlenfolge invers oder mit der gleichen Funktion verschlüsselt und mit der Zahlenfolge verglichen wird, und daß aus der Übereinstimmung der verglichenen Zahlenfolgen zumindest ein Teil des Selektionssignals abgeleitet wird.

4. Verfahren nach Anspruch 3,
dadurch gekennzeichnet, daß
das nach Feststellen der Übereinstimmung der verglichenen Zahlenfolgen von der Identifikationseinrichtung an die Steuereinrichtung übertragene Autorisierungssignal aus der Zahlenfolge oder der verschlüsselten Zahlenfolge durch weitere Verschlüsselung erzeugt wird und daß bei Übereinstimmung des in der Steuereinrichtung invers oder mit der gleichen Funktion verschlüsselten Autorisierungssignals der Identifika-tionseinrichtung mit der Zahlenfolge oder der verschlüsselten Zahlenfolge die Zugangskontrolleinrich-tung freigegeben wird.

5. Verfahren nach einem der Ansprüche 1 bis 4,
dadurch gekennzeichnet, daß
zumindest ein Teil des Selektionssignals als eine einer Identifikationseinrichtung zugeordneten Zahlenfolge übertragen wird.

6. Vorrichtung zur Prüfung der Nutzungsberechtigung für Zugangskontrolleinrichtungen, insbesondere für Schließeinrichtungen von Fahrzeugen, mit einer zugangsseitigen Steuereinrichtung und mit mindestens einer benutzerseitigen Identifikationseinrichtung, wobei zwischen der Steuereinrichtung und einer Identifikationseinrichtung Autorisierungssignale austauschbar sind und wobei die in Reichweite der Steuereinrichtung befindlichen Identifikationseinrichtungen automatisch zur Übertragung der Autorisierungssignale ansprechbar sind, insbesondere zur Verwirklichung eines Verfahrens nach einem der Ansprüche 1 bis 5,
dadurch gekennzeichnet, daß
die Steuereinrichtung ein Selektionssignal aussendet und daß eine Identifikationseinrichtung ein Autorisierungssignal nach dem Empfang eines ausschließlich dieser Identifikationseinrichtung zuzuordnenden Selektionssignals aussendet.

7. Vorrichtung nach Anspruch 6,
dadurch gekennzeichnet, daß
die Identifikationseinrichtung ein insbesondere als Transponder ausgebildeter Teil eines Fahrzeugschlüssels ist.

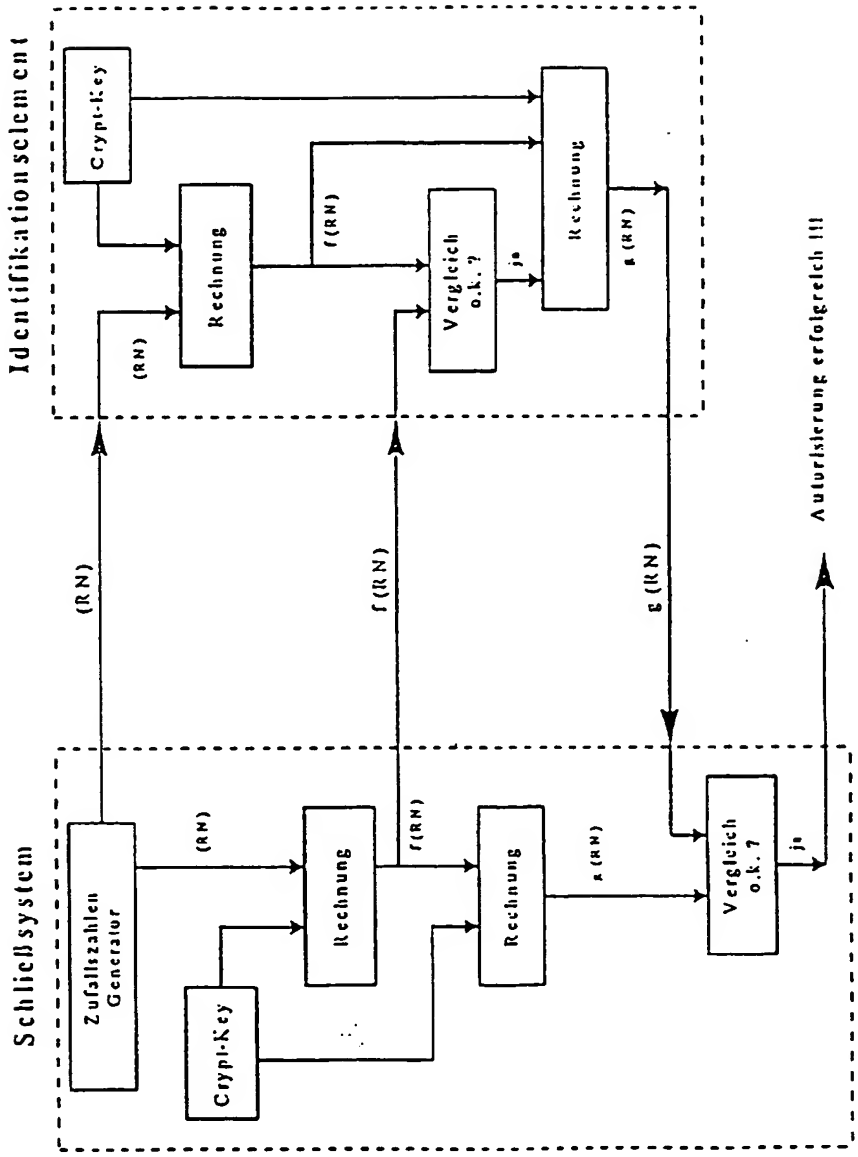

Fig. 1

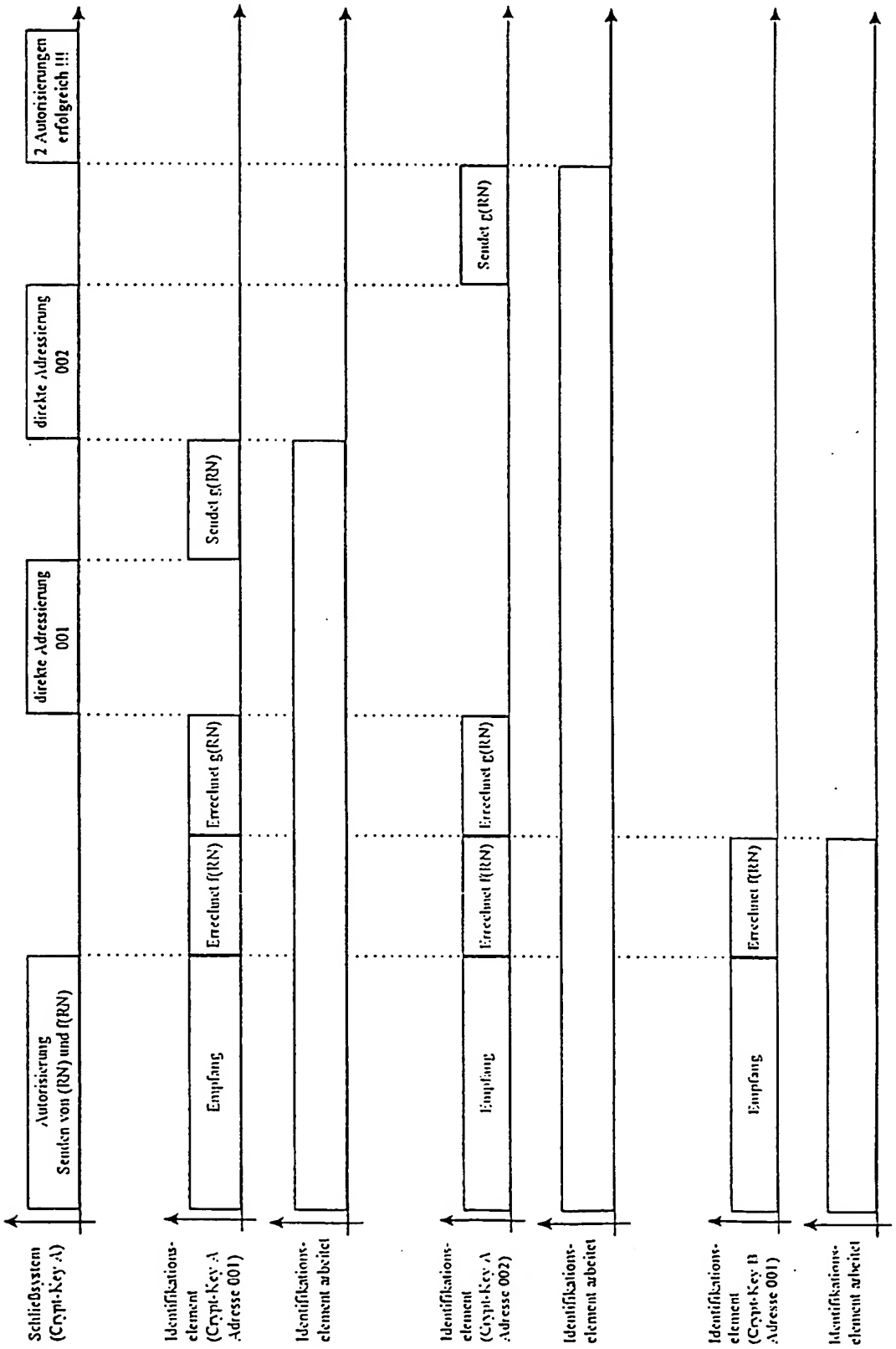

Fig. 2

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 923 054 A3

(12) EUROPÄISCHE PATENTANMELDUNG

(88) Veröffentlichungstag A3:
15.12.1999 Patentblatt 1999/50

(43) Veröffentlichungstag A2:
16.06.1999 Patentblatt 1999/24

(21) Anmeldenummer: **98122611.1**

(22) Anmeldetag: **27.11.1998**

(51) Int. Cl.[6]: **G07C 9/00**, E05B 49/00

(84) Benannte Vertragsstaaten:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Benannte Erstreckungsstaaten:
AL LT LV MK RO SI

(30) Priorität: **10.12.1997 DE 19754710**
06.04.1998 DE 19815300

(71) Anmelder:
F + G Megamos Sicherheitselektronik GMBH
51674 Wiehl (DE)

(72) Erfinder:
- **Petsching, Wilfried**
  51702 Bergneustadt (DE)
- **Marquart, Michael**
  59192 Bergkamen (DE)
- **Schenk, Christoph**
  51688 Wipperfürth (DE)
- **Seifert, Wolfgang**
  51647 Gummersbach-Lantenbach (DE)

(74) Vertreter: **Cohausz & Florack**
Patentanwälte
Kanzlerstrasse 8a
40472 Düsseldorf (DE)

(54) Verfahren und Vorrichtung zur Prüfung der Nutzungsberechtigung für Zugangskontrolleinrichtungen

(57) Die Erfindung betrifft ein Verfahren und eine Vorrichtung zur Prüfung der Nutzungsberechtigung für Zugangskontrolleinrichtungen und insbesondere für Schließeinrichtungen von Fahrzeugen, mit Hilfe einer zugangsseitigen Steuereinrichtung und mit Hilfe mindestens einer benutzerseitigen Identifikationseinrichtung, bei welchem zwischen der Steuereinrichung und einer Identifikationseinrichtung Autorisierungssignale ausgetauscht werden und bei welchem die in Reichweite der Steuereinrichtung befindlichen Identifikationseinrichtungen automatisch zur Übertragung der Autorisierungssignale angesprochen werden. Zur Vermeidung von Kollisionen der von verschiedenen Identifikationseinrichtungen übertragenen Autorisierungssignale ist vorgesehen, daß von der Steuereinrichtung ein Selektionssignal ausgesandt wird, und daß von einer Identifikationseinrichtung nach dem Empfang eines ausschließlich dieser Identifikationseinrichtung zuzuordnenden Selektionssignals das Autorisierungssignal ausgesendet wird.

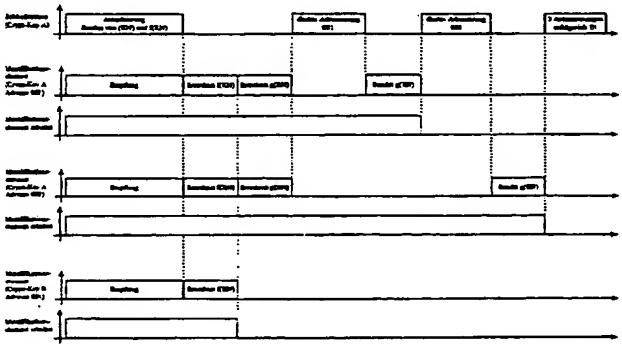

Fig. 2

EP 0 923 054 A3

Europäisches Patentamt

EUROPÄISCHER RECHERCHENBERICHT

Nummer der Anmeldung
EP 98 12 2611

EINSCHLÄGIGE DOKUMENTE

Kategorie	Kennzeichnung des Dokuments mit Angabe, soweit erforderlich, der maßgeblichen Teile	Betrifft Anspruch	KLASSIFIKATION DER ANMELDUNG (Int.Cl.6)
X Y	US 5 055 701 A (TAKEUCHI MIKIO) 8. Oktober 1991 (1991-10-08) * Zusammenfassung * * Spalte 1, Zeile 54 - Spalte 2, Zeile 61 * * Spalte 5, Zeile 7 - Zeile 63 * * Ansprüche 1-6; Abbildungen 1-4 *	1,2,5-7 3,4	G07C9/00 E05B49/00
X	EP 0 521 547 A (REGGIANI MEDARDO) 7. Januar 1993 (1993-01-07) * Zusammenfassung * * Seite 2, Zeile 30 - Seite 3, Zeile 6 * * Seite 8, Zeile 30 - Seite 9, Zeile 4 * * Abbildung 1 *	1,2,6,7	
X	GB 2 051 442 A (HOWARD J A) 14. Januar 1981 (1981-01-14) * Zusammenfassung * * Seite 1, Zeile 5 - Zeile 33 * * Seite 2, Zeile 4 - Seite 42 * * Abbildungen 1,2 *	1,2,6	
Y A	EP 0 739 109 A (UNITED TECHNOLOGIES AUTOMOTIVE) 23. Oktober 1996 (1996-10-23) * Zusammenfassung * * Seite 2, Zeile 32 - Zeile 40 * * Seite 2, Zeile 55 - Seite 3, Zeile 42 * * Abbildungen 1,2 *	3,4 1,6,7	RECHERCHIERTE SACHGEBIETE (Int.Cl.6) G07C E05B
A	SCHNEIDER C ET AL: "EIN FAHRZEUGSICHERUNGSSYSTEM OHNE MECHANISCHEN SCHLUESSEL VEHICLE SECURITY SYSTEM DISPENSING WITH MECHANICAL KEY" , ATZ AUTOMOBILTECHNISCHE ZEITSCHRIFT, VOL. 96, NR. 5, PAGE(S) 321 - 323, 330 XP000442154 ISSN: 0001-2785	1-7	

-/--

Der vorliegende Recherchenbericht wurde für alle Patentansprüche erstellt

Recherchenort	Abschlußdatum der Recherche	Prüfer
DEN HAAG	21. Oktober 1999	Miltgen, E

KATEGORIE DER GENANNTEN DOKUMENTE

X : von besonderer Bedeutung allein betrachtet
Y : von besonderer Bedeutung in Verbindung mit einer anderen Veröffentlichung derselben Kategorie
A : technologischer Hintergrund
O : nichtschriftliche Offenbarung
P : Zwischenliteratur

T : der Erfindung zugrunde liegende Theorien oder Grundsätze
E : älteres Patentdokument, das jedoch erst am oder nach dem Anmeldedatum veröffentlicht worden ist
D : in der Anmeldung angeführtes Dokument
L : aus anderen Gründen angeführtes Dokument

& : Mitglied der gleichen Patentfamilie, übereinstimmendes Dokument

EPO FORM 1503 03.82 (P04C03)

Europäisches Patentamt

EUROPÄISCHER RECHERCHENBERICHT

Nummer der Anmeldung
EP 98 12 2611

EINSCHLÄGIGE DOKUMENTE

Kategorie	Kennzeichnung des Dokuments mit Angabe, soweit erforderlich, der maßgeblichen Teile	Betrifft Anspruch	KLASSIFIKATION DER ANMELDUNG (Int.Cl.6)
A	GB 2 282 687 A (BRITISH TECH GROUP) 12. April 1995 (1995-04-12) * Zusammenfassung * * Seite 1, Zeile 26 - Seite 4, Zeile 24 * * Anspruch 1; Abbildungen 1,2 *	1,6,7	
A	EP 0 767 091 A (SIEMENS AG) 9. April 1997 (1997-04-09) * Zusammenfassung * * Spalte 1, Zeile 28 - Spalte 3, Zeile 22 * * Abbildung 1 *	1,6	
			RECHERCHIERTE SACHGEBIETE (Int.Cl.6)

Der vorliegende Recherchenbericht wurde für alle Patentansprüche erstellt

Recherchenort	Abschlußdatum der Recherche	Prüfer
DEN HAAG	21. Oktober 1999	Miltgen, E

KATEGORIE DER GENANNTEN DOKUMENTE

X : von besonderer Bedeutung allein betrachtet
Y : von besonderer Bedeutung in Verbindung mit einer anderen Veröffentlichung derselben Kategorie
A : technologischer Hintergrund
O : nichtschriftliche Offenbarung
P : Zwischenliteratur

T : der Erfindung zugrunde liegende Theorien oder Grundsätze
E : älteres Patentdokument, das jedoch erst am oder nach dem Anmeldedatum veröffentlicht worden ist
D : in der Anmeldung angeführtes Dokument
L : aus anderen Gründen angeführtes Dokument

& : Mitglied der gleichen Patentfamilie,übereinstimmendes Dokument

EPO FORM 1503 03.82 (P04C03)

ANHANG ZUM EUROPÄISCHEN RECHERCHENBERICHT ÜBER DIE EUROPÄISCHE PATENTANMELDUNG NR. EP 98 12 2611

In diesem Anhang sind die Mitglieder der Patentfamilien der im obengenannten europäischen Recherchenbericht angeführten Patentdokumente angegeben.
Die Angaben über die Familienmitglieder entsprechen dem Stand der Datei des Europäischen Patentamts am
Diese Angaben dienen nur zur Unterrichtung und erfolgen ohne Gewähr.

21-10-1999

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
US 5055701 A	08-10-1991	JP 2007099 C	11-01-1996
		JP 2051998 A	21-02-1990
		JP 7032499 B	10-04-1995
		DE 3927024 A	22-02-1990
EP 0521547 A	07-01-1993	IT 1253068 B	10-07-1995
		CA 2071603 A	02-01-1993
		US 5280267 A	18-01-1994
GB 2051442 A	14-01-1981	KEINE	
EP 0739109 A	23-10-1996	US 5598476 A	28-01-1997
GB 2282687 A	12-04-1995	AU 7817794 A	04-05-1995
		WO 9510432 A	20-04-1995
EP 0767091 A	09-04-1997	KEINE	

Für nähere Einzelheiten zu diesem Anhang : siehe Amtsblatt des Europäischen Patentamts, Nr.12/82